(Translation)

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application : April 6, 2000

Application Number : Patent Appln. No. 2000-105525

Applicant(s) : MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.

Wafer of the Patent Office

January 19, 2001

Kozo OIKAWA

Commissioner,
Patent Office

Seal of Commissioner of the Patent Office

Appln. Cert. No. Appln. Cert. Pat. 2000-3112877

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ４月 ６日

出 願 番 号
Application Number: 特願２０００－１０５５２５

出 願 人
Applicant (s): 松下電器産業株式会社

２００１年 １月１９日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２０００－３１１２８７７

【書類名】　特許願
【整理番号】　2022510411
【提出日】　平成12年 4月 6日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　柴田　修
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　関部　勉
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100078282
　【弁理士】
　【氏名又は名称】　山本　秀策
【手数料の表示】
　【予納台帳番号】　001878
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9303919
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　著作物保護システム、暗号化装置および復号化装置

【特許請求の範囲】

【請求項１】　コンテンツ鍵を用いて暗号通信を行う暗号化装置および復号化装置から構成される著作物保護システムであって、

前記暗号化装置は、コンテンツを記憶するコンテンツ記憶手段と、

第１解読制限を更新して得られる第２解読制限に基づいて前記コンテンツ鍵を生成する第１コンテンツ鍵生成手段と、

前記コンテンツを前記コンテンツ鍵に基づいて暗号化し、暗号化コンテンツを出力する第１暗号化手段とを具備し、

前記復号化装置は、前記第２解読制限から前記コンテンツ鍵を生成する第２コンテンツ鍵生成手段と、

前記暗号化コンテンツを前記第２コンテンツ鍵生成手段により生成された前記コンテンツ鍵を用いて復号化する第１復号化手段とを具備することを特徴とする著作物保護システム。

【請求項２】　前記復号化装置は、前記第１解読制限を解読制限更新則に基づいて前記第２解読制限に更新する解読制限更新手段と、

前記第２解読制限を時変鍵に基づいて暗号化し、第１暗号化解読制限を出力する第２暗号化手段とを具備し、

前記暗号化装置は、前記第２暗号化手段から転送される前記第１暗号化解読制限を前記時変鍵に基づいて復号化し、前記第２解読制限を生成する第２復号化手段とを具備し、

前記第１コンテンツ鍵生成手段は、前記第２復号化手段により生成された前記第２解読制限に基づいて前記コンテンツ鍵を生成する、請求項１記載の著作物保護システム。

【請求項３】　前記暗号化装置は、共通鍵を記憶する第１共通鍵記憶手段と、

前記第１解読制限を記憶する解読制限記憶手段と、

第１乱数を生成する第１乱数発生手段と、

前記第１乱数と前記復号化装置から転送される第２乱数とを用いて前記復号化装置と相互認証処理を行なう第１相互認証処理手段と、

前記第１相互認証処理手段における認証受理をうけて前記第１乱数と前記第２乱数とから前記時変鍵を生成する第１時変鍵生成手段と、

前記第１解読制限を前記時変鍵を用いて暗号化して第２暗号化解読制限を出力する第３暗号化手段とをさらに具備し、

前記復号化装置は、前記共通鍵を記憶する第２共通鍵記憶手段と、

前記第２乱数を生成する第２乱数発生手段と、

前記第２乱数と前記第１乱数とを用いて前記暗号化装置と相互認証を行なう第２相互認証処理手段と、

前記第２相互認証処理手段における認証受理をうけて前記第２乱数と前記第１乱数とから前記時変鍵を生成する第２時変鍵生成手段と、

前記第２暗号化解読制限を前記時変鍵を用いて復号化する第３復号化手段とを備える、請求項２記載の著作物保護システム。

【請求項４】　前記復号化装置は、前記第１解読制限を解読制限更新則に基づいて第２解読制限に更新する第１解読制限更新手段をさらに備え、

前記第２コンテンツ鍵生成手段は、前記第１解読制限更新手段により更新された前記第２解読制限に基づいて前記コンテンツ鍵を生成し、

前記暗号化装置は、前記復号化装置の第１解読制限更新手段における解読制限の更新をうけて、前記第１解読制限を解読制限更新則に従って前記第２解読制限に更新する第２解読制限更新手段をさらに備え、

前記第１コンテンツ鍵生成手段は、前記第２解読制限更新手段により更新された前記第２解読制限に基づいて前記コンテンツ鍵を生成する、請求項１記載の著作物保護システム。

【請求項５】　前記暗号化装置は、前記共通鍵を記憶する第１共通鍵記憶手段と、

前記第１解読制限を記憶する解読制限記憶手段と、

第１乱数を生成する第１乱数発生手段と、

前記第１乱数と前記復号化装置から転送される第２乱数とを用いて前記復号化

装置と相互認証を行なう第１相互認証処理手段と、

前記第１相互認証処理手段における認証受理をうけて前記第１乱数と前記第２乱数とから時変鍵を生成する第１時変鍵生成手段と、

前記第１解読制限を前記時変鍵を用いて暗号化して暗号化解読制限を出力する第２暗号化手段とを具備し、

前記復号化装置は、前記共通鍵を記憶する第２共通鍵記憶手段と、

前記第２乱数を生成する第２乱数発生手段と、

前記第２乱数と前記第１乱数とを用いて前記暗号化装置と相互認証を行なう第２相互認証処理手段と、

前記第２相互認証処理手段における認証受理をうけて前記第２乱数と前記第１乱数とから前記時変鍵を生成する第２時変鍵生成手段と、

前記暗号化解読制限を前記時変鍵を用いて復号化する第２復号化手段とを具備する、請求項４記載の著作物保護システム。

【請求項６】　前記第２解読制限更新手段は、予め前記第１解読制限を第２解読制限に更新し、

前記第２解読制限更新手段は、前記第１コンテンツ鍵生成手段に更新された前記第２解読制限を出力し、

前記第１コンテンツ鍵生成手段は、前記第２解読制限から前記コンテンツ鍵を生成し、

前記第２解読制限更新手段は、前記第１暗号化手段の処理が開始されたことをうけて、前記解読制限記憶手段に前記第２解読制限を格納する、請求項５記載の著作物保護システム。

【請求項７】　前記第１および第２時変鍵生成手段は、前記第１および第２乱数と前記共通鍵に基づいて前記時変鍵を生成する、請求項３記載の著作物保護システム。

【請求項８】　前記第１および第２コンテンツ鍵生成手段は、前記第２解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成する、請求項３記載の著作物保護システム。

【請求項９】　前記暗号化装置および前記復号化装置は、前記暗号化装置お

よび前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第１および第２データ系列鍵生成手段をそれぞれさらに具備し、

前記第１および第２時変鍵生成手段は、前記第１および第２乱数と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項３記載の著作物保護システム。

【請求項１０】　前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第１および第２データ系列鍵生成手段をそれぞれさらに具備し、

前記第１および第２時変鍵生成手段は、前記第１および第２乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項３記載の著作物保護システム。

【請求項１１】　前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第１および第２データ系列鍵生成手段をそれぞれさらに具備し、

前記第１および第２コンテンツ鍵生成手段は、前記第２解読制限と前記データ系列鍵に基づいて前記コンテンツ生成鍵を生成する、請求項３記載の著作物保護システム。

【請求項１２】　前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第１および第２データ系列鍵生成手段をそれぞれさらに具備し、

前記第１および第２コンテンツ鍵生成手段は、前記第２解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成する、請求項３記載の著作物保護システム。

【請求項１３】　前記第１および第２相互認証処理手段は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証する、請求項３記載の著作物保護システム。

【請求項１４】　コンテンツ鍵を用いて復号化装置と暗号通信を行う暗号化装置であって、

前記暗号化装置は、コンテンツを記憶するコンテンツ記憶手段と、

第１解読制限を更新して得られる第２解読制限に基づいて前記コンテンツ鍵を生成するコンテンツ鍵生成手段と、

前記コンテンツを前記コンテンツ鍵に基づいて暗号化し、暗号化コンテンツを出力する第１暗号化手段とを具備することを特徴とする暗号化装置。

【請求項１５】　前記暗号化装置は、前記復号化装置から転送される第１暗号化解読制限を時変鍵に基づいて復号化し、前記第２解読制限を生成する復号化手段を具備し、

前記コンテンツ鍵生成手段は、前記復号化手段により生成された前記第２解読制限に基づいて前記コンテンツ鍵を生成する、請求項１４記載の暗号化装置。

【請求項１６】　前記暗号化装置は、共通鍵を記憶する共通鍵記憶手段と、

前記第１解読制限を記憶する解読制限記憶手段と、

第１乱数を生成する第１乱数発生手段と、

前記第１乱数と前記復号化装置から転送される第２乱数とを用いて前記復号化装置と相互認証処理を行なう相互認証処理手段と、

前記相互認証処理手段における認証受理をうけて前記第１乱数と前記第２乱数とから前記時変鍵を生成する時変鍵生成手段と、

前記第１解読制限を前記時変鍵を用いて暗号化して第２暗号化解読制限を出力する第２暗号化手段とをさらに具備する、請求項１５記載の暗号化装置。

【請求項１７】　前記暗号化装置は、前記復号化装置の解読制限の更新をうけて、前記第１解読制限を解読制限更新則に従って前記第２解読制限に更新する解読制限更新手段をさらに備え、

前記コンテンツ鍵生成手段は、前記解読制限更新手段により更新された前記第２解読制限に基づいて前記コンテンツ鍵を生成する、請求項１４記載の暗号化装置。

【請求項１８】　前記暗号化装置は、前記共通鍵を記憶する共通鍵記憶手段と、

前記第１解読制限を記憶する解読制限記憶手段と、

第１乱数を生成する第１乱数発生手段と、

前記第１乱数と前記復号化装置から転送される第２乱数とを用いて前記復号化

装置と相互認証を行なう相互認証処理手段と、

前記相互認証処理手段における認証受理をうけて前記第１乱数と前記第２乱数とから時変鍵を生成する時変鍵生成手段と、

前記第１解読制限を前記時変鍵を用いて暗号化して暗号化解読制限を出力する第２暗号化手段とを具備する、請求項１７記載の暗号化装置。

【請求項１９】　前記解読制限更新手段は、予め前記第１解読制限を第２解読制限に更新し、

前記解読制限更新手段は、前記コンテンツ鍵生成手段に更新された前記第２解読制限を出力し、

前記コンテンツ鍵生成手段は、前記第２解読制限から前記コンテンツ鍵を生成し、

前記解読制限更新手段は、前記第１暗号化手段の処理が開始されたことをうけて、前記解読制限記憶手段に前記第２解読制限を格納する、請求項１８記載の暗号化装置。

【請求項２０】　前記時変鍵生成手段は、前記第１および第２乱数と前記共通鍵に基づいて前記時変鍵を生成する、請求項１６記載の暗号化装置。

【請求項２１】　前記コンテンツ鍵生成手段は、前記第２解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成する、請求項１６記載の暗号化装置。

【請求項２２】　前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記時変鍵生成手段は、前記第１および第２乱数と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項１６記載の暗号化装置。

【請求項２３】　前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記時変鍵生成手段は、前記第１および第２乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項１６記載の暗号化装置。

【請求項２４】　前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記コンテンツ鍵生成手段は、前記第２解読制限と前記データ系列鍵に基づい

て前記コンテンツ生成鍵を生成する、請求項１６記載の暗号化装置。

【請求項２５】　前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記コンテンツ鍵生成手段は、前記第２解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成する、請求項１６記載の暗号化装置。

【請求項２６】　コンテンツ鍵を用いて暗号化装置と暗号通信を行う復号化装置であって、

前記復号化装置は、第２解読制限から前記コンテンツ鍵を生成するコンテンツ鍵生成手段と、

暗号化コンテンツを前記コンテンツ鍵生成手段により生成された前記コンテンツ鍵を用いて復号化する第１復号化手段とを具備することを特徴とする復号化装置。

【請求項２７】　前記復号化装置は、前記第１解読制限を解読制限更新則に基づいて前記第２解読制限に更新する解読制限更新手段と、

前記第２解読制限を時変鍵に基づいて暗号化し、第１暗号化解読制限を出力する暗号化手段とを具備する、請求項２６記載の復号化装置。

【請求項２８】　前記復号化装置は、前記共通鍵を記憶する共通鍵記憶手段と、

前記第２乱数を生成する乱数発生手段と、

前記第２乱数と第１乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段と、

前記相互認証処理手段における認証受理をうけて前記第２乱数と前記第１乱数とから前記時変鍵を生成する時変鍵生成手段と、

第１暗号化解読制限を前記時変鍵を用いて復号化する第２復号化手段とを備える、請求項２７記載の復号化装置。

【請求項２９】　前記復号化装置は、前記第１解読制限を解読制限更新則に基づいて第２解読制限に更新する解読制限更新手段をさらに備え、

前記コンテンツ鍵生成手段は、前記解読制限更新手段により更新された前記第

２解読制限に基づいて前記コンテンツ鍵を生成する、請求項２６記載の復号化装置。

【請求項３０】　前記復号化装置は、前記共通鍵を記憶する第２共通鍵記憶手段と、

前記第２乱数を生成する第２乱数発生手段と、

前記第２乱数と第１乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段と、

前記相互認証処理手段における認証受理をうけて前記第２乱数と前記第１乱数とから前記時変鍵を生成する時変鍵生成手段と、

暗号化解読制限を前記時変鍵を用いて復号化する第２復号化手段とを具備する、請求項２９記載の復号化装置。

【請求項３１】　前記時変鍵生成手段は、前記第１および第２乱数と前記共通鍵に基づいて前記時変鍵を生成する、請求項２８記載の復号化装置。

【請求項３２】　前記コンテンツ鍵生成手段は、前記第２解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成する、請求項２８記載の復号化装置。

【請求項３３】　前記前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記時変鍵生成手段は、前記第１および第２乱数と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項２８記載の復号化装置。

【請求項３４】　前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記時変鍵生成手段は、前記第１および第２乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項２８記載の復号化装置。

【請求項３５】　前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記コンテンツ鍵生成手段は、前記第２解読制限と前記データ系列鍵に基づいて前記コンテンツ生成鍵を生成する、請求項２８記載の復号化装置。

【請求項３６】　前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記コンテンツ鍵生成手段は、前記第２解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成する、請求項２８記載の復号化装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、解読制限を持った音楽、画像、映像、ゲームなどのディジタルコンテンツを機器間で共通鍵を共有化して暗号通信を行う通信システムにおいて、解読制限の更新が不正に行われた場合に解読できないようにしたものであり、共通鍵に解読制限の更新情報を関連させることによって著作物を保護するシステムに関する。

【０００２】

【従来の技術】

近年、ディジタル情報圧縮技術の進展とインターネットに代表されるグローバルな通信インフラの爆発的な普及によって音楽、画像、映像、ゲームなどのコンテンツをディジタル情報として通信回線を利用して各家庭に配信することが実現されはじめた。

【０００３】

通信回線を利用したディジタル情報の配信サービスは、媒体によらないデータだけの流通形態であるため、配信サービス形態の自由度が飛躍的に向上し、単にコンテンツ情報を配信するだけでなく、使用回数、使用期間などの使用制限付きで配信させるなど、多用な形態で流通させることが可能である。

【０００４】

ディジタルコンテンツの著作権者の権利や流通業者の利益を保護した流通配信システムを確立するために、通信の傍受、盗聴、なりすましなどによる不正入手や、受信したデータを記憶した記録媒体における違法複製、違法改ざんなどの不正行為を防止することが課題となり、正規システムの判別、データスクランブルを行なう暗号／認証などの著作物保護技術が必要となる。

【０００５】

著作物保護技術については従来より種々なものが知られており、代表的なものとしてデータの暗号化装置と復号化装置間で乱数、応答値の交換を行ない相互に正当性を認証し合い、正当である場合のみデータを送信するチャレンジレスポンス型の相互認証技術がある。

【０００６】

本明細書において「解読制限」とは、暗号化装置から復号化装置に転送されたコンテンツを使用（再生して音をだすとか）してよいかの情報を意味する。例えば、再生回数付きのコンテンツの場合、解読制限は回数情報である。

【０００７】

「解読制限の更新」とは、解読制限の更新則を意味する。例えば、再生回数付きのコンテンツの場合、暗号化装置から復号化装置に転送される解読制限（Ｎ回使用可能）の回数情報を１つ減らすことを意味する。

【０００８】

「解読制限の更新情報」とは、更新された解読制限を意味する。例えば、再生回数付きのコンテンツの場合、暗号化装置から復号化装置に転送される解読制限（Ｎ回使用可能）が、解読制限の更新によって、解読制限の回数情報が「Ｎ－１回使用可能」と書きかえられた情報をさす。

【０００９】

特に解読制限を持ったディジタルコンテンツを、前述の相互認証技術を用いて暗号通信を行なうシステムを考えた場合、データの暗号化装置と復号化装置間で相互に正当性を認証し合い、正当であると確認された時のみ解読制限を暗号化装置から復号化装置に暗号通信で転送し、復号化装置は解読制限を解釈して解読可能であるかを判定するとともに解読制限の更新情報を暗号化装置に暗号通信で送信したのち、コンテンツデータを暗号化装置から暗号通信でロードし解読して使用するのが一般的に行なわれる方法である。

【００１０】

【発明が解決しようとする課題】

ここで課題となるのは、解読制限を記憶している解読制限の更新が正常に行なわれることであり、解読制限の更新が正常に行なわれていない場合、コンテンツ

を解読できないシステムが必要となる。

【００１１】

前述の相互認証技術では、通信する機器が正規なものかを判定するだけであり、必ずしも解読制限の更新が正常に行なわれたかを判定し、不正行為を防止するものではなく、解読制限の更新情報の転送のみを別の機器になりすまされた場合、問題となる。例えば、前述のシステムにおいて解読制限の更新情報の転送のみを別の機器になりすまされて処理された場合を考えると、解読制限の更新情報を復号化装置で暗号化して転送しても、転送先が正規の暗号化装置ではなく別の暗号化装置がなりすまして処理した場合、正規の暗号化装置では解読制限の更新がなされないことになる。

【００１２】

本発明の目的は、解読制限の更新を確実に行なうとともに、ディジタルコンテンツの不正解読を防止するシステムを提供することにある。

【００１３】

【課題を解決するための手段】

本発明に係る著作物保護システムは、コンテンツ鍵を用いて暗号通信を行う暗号化装置および復号化装置から構成される著作物保護システムであって、前記暗号化装置は、コンテンツを記憶するコンテンツ記憶手段と、第１解読制限を更新して得られる第２解読制限に基づいて前記コンテンツ鍵を生成する第１コンテンツ鍵生成手段と、前記コンテンツを前記コンテンツ鍵に基づいて暗号化し、暗号化コンテンツを出力する第１暗号化手段とを具備し、前記復号化装置は、前記第２解読制限から前記コンテンツ鍵を生成する第２コンテンツ鍵生成手段と、前記暗号化コンテンツを前記第２コンテンツ鍵生成手段により生成された前記コンテンツ鍵を用いて復号化する第１復号化手段とを具備することを特徴とし、そのことにより上記目的が達成される。

【００１４】

前記復号化装置は、前記第１解読制限を解読制限更新則に基づいて前記第２解読制限に更新する解読制限更新手段と、前記第２解読制限を時変鍵に基づいて暗号化し、第１暗号化解読制限を出力する第２暗号化手段とを具備し、前記暗号化

装置は、前記第２暗号化手段から転送される前記第１暗号化解読制限を前記時変鍵に基づいて復号化し、前記第２解読制限を生成する第２復号化手段とを具備し、前記第１コンテンツ鍵生成手段は、前記第２復号化手段により生成された前記第２解読制限に基づいて前記コンテンツ鍵を生成してもよい。

【００１５】

前記暗号化装置は、共通鍵を記憶する第１共通鍵記憶手段と、前記第１解読制限を記憶する解読制限記憶手段と、第１乱数を生成する第１乱数発生手段と、前記第１乱数と前記復号化装置から転送される第２乱数とを用いて前記復号化装置と相互認証処理を行なう第１相互認証処理手段と、前記第１相互認証処理手段における認証受理をうけて前記第１乱数と前記第２乱数とから前記時変鍵を生成する第１時変鍵生成手段と、前記第１解読制限を前記時変鍵を用いて暗号化して第２暗号化解読制限を出力する第３暗号化手段とをさらに具備し、前記復号化装置は、前記共通鍵を記憶する第２共通鍵記憶手段と、前記第２乱数を生成する第２乱数発生手段と、前記第２乱数と前記第１乱数とを用いて前記暗号化装置と相互認証を行なう第２相互認証処理手段と、前記第２相互認証処理手段における認証受理をうけて前記第２乱数と前記第１乱数とから前記時変鍵を生成する第２時変鍵生成手段と、前記第２暗号化解読制限を前記時変鍵を用いて復号化する第３復号化手段とを備えてもよい。

【００１６】

前記復号化装置は、前記第１解読制限を解読制限更新則に基づいて第２解読制限に更新する第１解読制限更新手段をさらに備え、前記第２コンテンツ鍵生成手段は、前記第１解読制限更新手段により更新された前記第２解読制限に基づいて前記コンテンツ鍵を生成し、前記暗号化装置は、前記復号化装置の第１解読制限更新手段における解読制限の更新をうけて、前記第１解読制限を解読制限更新則に従って前記第２解読制限に更新する第２解読制限更新手段をさらに備え、前記第１コンテンツ鍵生成手段は、前記第２解読制限更新手段により更新された前記第２解読制限に基づいて前記コンテンツ鍵を生成してもよい。

【００１７】

前記暗号化装置は、前記共通鍵を記憶する第１共通鍵記憶手段と、前記第１解

読制限を記憶する解読制限記憶手段と、第１乱数を生成する第１乱数発生手段と、前記第１乱数と前記復号化装置から転送される第２乱数とを用いて前記復号化装置と相互認証を行なう第１相互認証処理手段と、前記第１相互認証処理手段における認証受理をうけて前記第１乱数と前記第２乱数とから時変鍵を生成する第１時変鍵生成手段と、前記第１解読制限を前記時変鍵を用いて暗号化して暗号化解読制限を出力する第２暗号化手段とを具備し、前記復号化装置は、前記共通鍵を記憶する第２共通鍵記憶手段と、前記第２乱数を生成する第２乱数発生手段と、前記第２乱数と前記第１乱数とを用いて前記暗号化装置と相互認証を行なう第２相互認証処理手段と、前記第２相互認証処理手段における認証受理をうけて前記第２乱数と前記第１乱数とから前記時変鍵を生成する第２時変鍵生成手段と、前記暗号化解読制限を前記時変鍵を用いて復号化する第２復号化手段とを具備し、そのことにより上記目的が達成される。

【００１８】

前記第２解読制限更新手段は、予め前記第１解読制限を第２解読制限に更新し、前記第２解読制限更新手段は、前記第１コンテンツ鍵生成手段に更新された前記第２解読制限を出力し、前記第１コンテンツ鍵生成手段は、前記第２解読制限から前記コンテンツ鍵を生成し、前記第２解読制限更新手段は、前記第１暗号化手段の処理が開始されたことをうけて、前記解読制限記憶手段に前記第２解読制限を格納してもよい。

【００１９】

前記第１および第２時変鍵生成手段は、前記第１および第２乱数と前記共通鍵に基づいて前記時変鍵を生成してもよい。

【００２０】

前記第１および第２コンテンツ鍵生成手段は、前記第２解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成してもよい。

【００２１】

前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第１および第２データ系列鍵生成手段をそれぞれさらに具備し、前記第１および第２時変鍵生成手段は

、前記第１および第２乱数と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

【００２２】

前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第１および第２データ系列鍵生成手段をそれぞれさらに具備し、前記第１および第２時変鍵生成手段は、前記第１および第２乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

【００２３】

前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第１および第２データ系列鍵生成手段をそれぞれさらに具備し、前記第１および第２コンテンツ鍵生成手段は、前記第２解読制限と前記データ系列鍵に基づいて前記コンテンツ生成鍵を生成してもよい。

【００２４】

前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第１および第２データ系列鍵生成手段をそれぞれさらに具備し、前記第１および第２コンテンツ鍵生成手段は、前記第２解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成してもよい。

【００２５】

前記第１および第２相互認証処理手段は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証してもよい。

【００２６】

本発明に係る暗号化装置は、コンテンツ鍵を用いて復号化装置と暗号通信を行う暗号化装置であって、前記暗号化装置は、コンテンツを記憶するコンテンツ記憶手段と、第１解読制限を更新して得られる第２解読制限に基づいて前記コンテンツ鍵を生成するコンテンツ鍵生成手段と、前記コンテンツを前記コンテンツ鍵

に基づいて暗号化し、暗号化コンテンツを出力する第１暗号化手段とを具備し、そのことにより上記目的が達成される。

【００２７】

前記暗号化装置は、前記復号化装置から転送される第１暗号化解読制限を時変鍵に基づいて復号化し、前記第２解読制限を生成する復号化手段を具備し、前記コンテンツ鍵生成手段は、前記復号化手段により生成された前記第２解読制限に基づいて前記コンテンツ鍵を生成してもよい。

【００２８】

前記暗号化装置は、共通鍵を記憶する共通鍵記憶手段と、前記第１解読制限を記憶する解読制限記憶手段と、第１乱数を生成する第１乱数発生手段と、前記第１乱数と前記復号化装置から転送される第２乱数とを用いて前記復号化装置と相互認証処理を行なう相互認証処理手段と、前記相互認証処理手段における認証受理をうけて前記第１乱数と前記第２乱数とから前記時変鍵を生成する時変鍵生成手段と、前記第１解読制限を前記時変鍵を用いて暗号化して第２暗号化解読制限を出力する第２暗号化手段とをさらに具備してもよい。

【００２９】

前記暗号化装置は、前記復号化装置の解読制限の更新をうけて、前記第１解読制限を解読制限更新則に従って前記第２解読制限に更新する解読制限更新手段をさらに備え、前記コンテンツ鍵生成手段は、前記解読制限更新手段により更新された前記第２解読制限に基づいて前記コンテンツ鍵を生成してもよい。

【００３０】

前記暗号化装置は、前記共通鍵を記憶する共通鍵記憶手段と、前記第１解読制限を記憶する解読制限記憶手段と、第１乱数を生成する第１乱数発生手段と、前記第１乱数と前記復号化装置から転送される第２乱数とを用いて前記復号化装置と相互認証を行なう相互認証処理手段と、前記相互認証処理手段における認証受理をうけて前記第１乱数と前記第２乱数とから時変鍵を生成する時変鍵生成手段と、前記第１解読制限を前記時変鍵を用いて暗号化して暗号化解読制限を出力する第２暗号化手段とを具備してもよい。

【００３１】

前記解読制限更新手段は、予め前記第１解読制限を第２解読制限に更新し、前記解読制限更新手段は、前記コンテンツ鍵生成手段に更新された前記第２解読制限を出力し、前記コンテンツ鍵生成手段は、前記第２解読制限から前記コンテンツ鍵を生成し、前記解読制限更新手段は、前記第１暗号化手段の処理が開始されたことをうけて、前記解読制限記憶手段に前記第２解読制限を格納してもよい。

【００３２】

前記時変鍵生成手段は、前記第１および第２乱数と前記共通鍵に基づいて前記時変鍵を生成してもよい。

【００３３】

前記コンテンツ鍵生成手段は、前記第２解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成してもよい。

【００３４】

前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記時変鍵生成手段は、前記第１および第２乱数と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

【００３５】

前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記時変鍵生成手段は、前記第１および第２乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

【００３６】

前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記コンテンツ鍵生成手段は、前記第２解読制限と前記データ系列鍵に基づいて前記コンテンツ生成鍵を生成してもよい。

【００３７】

前記暗号化装置は、前記暗号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記コンテンツ鍵生成手段

は、前記第２解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成してもよい。

【００３８】

本発明に係る復号化装置は、コンテンツ鍵を用いて暗号化装置と暗号通信を行う復号化装置であって、前記復号化装置は、第２解読制限から前記コンテンツ鍵を生成するコンテンツ鍵生成手段と、暗号化コンテンツを前記コンテンツ鍵生成手段により生成された前記コンテンツ鍵を用いて復号化する第１復号化手段とを具備し、そのことにより上記目的が達成される。

【００３９】

前記復号化装置は、前記第１解読制限を解読制限更新則に基づいて前記第２解読制限に更新する解読制限更新手段と、前記第２解読制限を時変鍵に基づいて暗号化し、第１暗号化解読制限を出力する暗号化手段とを具備してもよい。

【００４０】

前記復号化装置は、前記共通鍵を記憶する共通鍵記憶手段と、前記第２乱数を生成する乱数発生手段と、前記第２乱数と第１乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段と、前記相互認証処理手段における認証受理をうけて前記第２乱数と前記第１乱数とから前記時変鍵を生成する時変鍵生成手段と、第１暗号化解読制限を前記時変鍵を用いて復号化する第２復号化手段とを備えてもよい。

【００４１】

前記復号化装置は、前記第１解読制限を解読制限更新則に基づいて第２解読制限に更新する解読制限更新手段をさらに備え、前記コンテンツ鍵生成手段は、前記解読制限更新手段により更新された前記第２解読制限に基づいて前記コンテンツ鍵を生成してもよい。

【００４２】

前記復号化装置は、前記共通鍵を記憶する第２共通鍵記憶手段と、前記第２乱数を生成する第２乱数発生手段と、前記第２乱数と第１乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段と、前記相互認証処理手段における認証受理をうけて前記第２乱数と前記第１乱数とから前記時変鍵を生成する時変

鍵生成手段と、暗号化解読制限を前記時変鍵を用いて復号化する第２復号化手段とを具備してもよい。

【００４３】

前記時変鍵生成手段は、前記第１および第２乱数と前記共通鍵に基づいて前記時変鍵を生成してもよい。

【００４４】

前記コンテンツ鍵生成手段は、前記第２解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成してもよい。

【００４５】

前記前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記時変鍵生成手段は、前記第１および第２乱数と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

【００４６】

前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記時変鍵生成手段は、前記第１および第２乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

【００４７】

前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記コンテンツ鍵生成手段は、前記第２解読制限と前記データ系列鍵に基づいて前記コンテンツ生成鍵を生成してもよい。

【００４８】

前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記コンテンツ鍵生成手段は、前記第２解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成してもよい。

【００４９】

本発明では、ディジタルコンテンツの暗号通信に用いる共通鍵の生成に解読制限を用いる。

【００５０】

【発明の実施の形態】

以下に本発明の原理と実施の形態を添付の図面を用いて説明する。

【００５１】

（実施の形態１）

図１は、本発明の実施の形態１における構成図を示し暗号化装置１０１と復号化装置１０２が暗号通信を行なうシステム１００を示す。

【００５２】

暗号化装置１０１は、共通鍵ＵＫを記憶する共通鍵記憶部１０３と、解読制限を記憶する解読制限記憶部１１１と、コンテンツＣＴを記憶するコンテンツ記憶部１２１と、乱数Ｒ１を生成する乱数発生部１０５と、乱数Ｒ１と復号化装置１０２から転送される乱数Ｒ２と共通鍵ＵＫとを用いて復号化装置１０２と相互認証処理を行なう相互認証処理部１０７と、相互認証処理部１０７における相互認証処理に応答して乱数Ｒ１と乱数Ｒ２とから相互認証処理が実行される度に可変な時変鍵ＶＫを生成する時変鍵生成部１０９と、解読制限Ｓ１を時変鍵ＶＫを用いて暗号化して暗号化解読制限Ｓ２を出力する暗号化部１１３と、復号化装置１０２の暗号化部１１６から転送される暗号化解読制限Ｓ３を時変鍵ＶＫを用い解読制限Ｓ４に復号化し、解読制限記憶部１１１に書き込む復号化部１１５と、解読制限Ｓ４からコンテンツ鍵ＣＫを生成するコンテンツ鍵生成部１１７と、コンテンツＣＴをコンテンツ鍵ＣＫに基づいて暗号化し、暗号化コンテンツＳ５を出力する暗号化部１１９とを備える。

【００５３】

復号化装置１０２は、共通鍵ＵＫを記憶する共通鍵記憶部１０４と、乱数Ｒ２を生成する乱数発生部１０６と、乱数Ｒ２と乱数Ｒ１と共通鍵ＵＫを用いて暗号化装置１０１と相互認証処理を行なう相互認証処理部１０８と、相互認証処理部１０８における相互認証処理に応答して乱数Ｒ２と乱数Ｒ１とから時変鍵ＶＫを生成する時変鍵生成部１１０と、暗号化解読制限Ｓ２を時変鍵ＶＫを用いて復号

化する復号化部１１４と、復号化部１１４で復号化した解読制限Ｓ１を解読制限更新則に基づいて解読制限Ｓ４に更新する解読制限更新部１１２と、解読制限Ｓ４を時変鍵ＶＫを用いて暗号化し、暗号化解読制限Ｓ３を出力する暗号化部１１６と、解読制限Ｓ４からコンテンツ鍵ＣＫを生成するコンテンツ鍵生成部１１８と、暗号化コンテンツＳ５をコンテンツ鍵ＣＫを用いて復号化し、コンテンツＣＴを出力する復号化部１２０とを備える。

【００５４】

暗号化装置１０１、復号化装置１０２はともに共通鍵記憶部１０３、１０４を備え同一の共通化鍵ＵＫを保持する。尚、予め共通化鍵ＵＫは同一共通鍵として共通鍵記憶部１０３、１０４に記憶されていてもよいし、作成プロセスにより同一の共通化鍵ＵＫを作成してもよい。

【００５５】

暗号化装置１０１は、解読制限Ｓ１を記憶する解読制限記憶部１１１とコンテンツＣＴを記憶するコンテンツ記憶部１２１を備える。なお、これら共通鍵記憶部１０３、解読制限記憶部１１１、コンテンツ記憶部１２１は外部から直接アクセスすることができないプロテクト領域に配置されている。

【００５６】

以下図１および図２を参照して、暗号化装置１０１と復号化装置１０２とを含むシステム１００の処理手順を説明する。

【００５７】

暗号化装置１０１、復号化装置１０２は、互いに独立に乱数Ｒ１、Ｒ２を発生する乱数発生部１０５、１０６を備え、互いの乱数Ｒ１、Ｒ２を交換し、乱数Ｒ１と共通化鍵ＵＫを用いて応答値Ｖ１を作成し、乱数Ｒ２と共通化鍵ＵＫを用いて応答値Ｖ２を作成し、応答値Ｖ１、Ｖ２を交換し、比較することによって相互に相手機器が正当な機器であることを認証するチャレンジレスポンス型の相互認証を相互認証処理部１０７、１０８で行なう（Ｓ２０１）。

【００５８】

相互認証処理部１０７、１０８によって相手機器が正当であることを確認する認証確立が成立したか否かが判断される（Ｓ２０２）。認証確立が成立しないと

判断された場合には（Ｓ２０２でＮＯ）、処理は終了する。認証確立が成立したと判断された場合には（Ｓ２０２でＹＥＳ）、時変鍵生成部１０９、１１０は互いの乱数Ｒ１、Ｒ２から相互認証毎に変化する同一の時変鍵ＶＫを生成する（Ｓ２０３）。その後、暗号化装置１０１内の解読制限記憶部１１１に格納されている解読制限Ｓ１を時変鍵ＶＫを用いて暗号化部１１３で暗号化して暗号化解読制限Ｓ２を復号化装置１０２に転送する（Ｓ２０４）。

【００５９】

復号化部１１４は受信した暗号化解読制限Ｓ２を同じく時変鍵ＶＫを用いて復号化する（Ｓ２０５）。復号化部１１４にて復号化された解読制限Ｓ１を解読制限更新部１１２は解読制限更新則に従って更新し（Ｓ２０６）、更新された解読制限Ｓ４を時変鍵ＶＫを用いて暗号化して（Ｓ２０７）暗号化解読制限Ｓ３を暗号化装置１０１に転送する。復号化部１１５は、転送された暗号化解読制限Ｓ３を時変鍵ＶＫを用いて復号化して更新された解読制限Ｓ４を得て、解読制限記憶部１１１に格納する（Ｓ２０８）。

【００６０】

コンテンツ鍵生成部１１７は解読制限Ｓ４からコンテンツ鍵ＣＫを生成する（Ｓ２０９）。コンテンツ記憶部１２１に格納されているコンテンツＣＴを暗号化装置１０１から復号化装置１０２に転送する場合、暗号化部１１９はコンテンツ鍵ＣＫを用いてコンテンツＣＴを暗号化する（Ｓ２１０）。コンテンツ鍵生成部１１８は解読制限Ｓ４からコンテンツ鍵ＣＫを生成する（Ｓ２１１）。復号化装置内復号化部１２０はコンテンツ鍵ＣＫを用いて暗号化コンテンツＳ５を復号する（Ｓ２１２）。

【００６１】

なお、本実施の形態では、１回の認証確立後コンテンツを暗号化装置から復号化装置に転送する例を示したが、認証確立後、送復号化装置間でコンテンツ転送が発生する毎に相手機器が正当であることを確認する相互認証を行うようにしてもよい。また、時変鍵ＶＫの生成に、相互認証に用いた乱数Ｒ１、Ｒ２を用いたが、応答値Ｖ１、Ｖ２を用いてもかまわない。

【００６２】

また、解読制限、コンテンツの暗号化および復号化に用いる方法は異なるアルゴリズムでも同一のアルゴリズムのものを用いてよく、例えばＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）などを用いればよい。

【００６３】

また、時変鍵、コンテンツ鍵の生成に用いる方法は異なるアルゴリズムでも同一のアルゴリズムのものを用いてよく、例えばＳＨＡ（Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ）などの一方向性の関数を用いればよい。

【００６４】

なお本実施の形態では本発明を分かりやすく説明するために、送受信を相互認証処理部１０７、１０８、暗号化部１１３、復号化部１１４、復号化部１１５、暗号化部１１６、暗号化部１１９、復号化部１２０が行っている例を示しているが。実際の送受信は、制御部１２２、１２３で管理されることが一般的である。後述する実施の形態でも同様である。

【００６５】

以上のように、本実施の形態の著作物保護システムは、著作物であるコンテンツＣＴの転送において、解読制限の更新情報（解読制限Ｓ４）を関連させてコンテンツの暗号通信を行うので、正しく解読制限Ｓ１の更新処理を行わないと、コンテンツＣＴを解読できないという効果がある。

【００６６】

（実施の形態２）

図２は、本発明の実施の形態２における著作物保護システム２００を示す。図２において図１と同一の構成要素には同一の参照符号を付し、説明を省略する。

【００６７】

著作物保護システム２００では、図１で示した著作物保護システム１００のように解読制限更新部１１２で更新された解読制限Ｓ４を暗号化／復号化を行なって転送し、解読制限記憶部１１１に格納するのではなく、暗号化装置２０１内にも解読制限更新部２２３を備える。

【００６８】

復号化装置２０２の解読制限更新部２１２は、解読制限Ｓ１の更新を命令する

解読制限更新指令ＣＣだけを解読制限更新部２２３に転送する。解読制限更新部２２３は転送される解読制限更新指令ＣＣを受けとり、解読制限Ｓ１を更新し、更新した解読制限Ｓ４を解読制限記憶部２１１に格納する。

【００６９】

以上のように、本実施の形態の著作物保護システム２００は、コンテンツ鍵ＣＫの生成に関連する更新された解読制限Ｓ４を復号化装置２０２から暗号化装置２０１へ転送する必要がないため、解読制限Ｓ４の秘匿性を高めることができる。また、更新された解読制限Ｓ４の転送に係わる暗号化部、復号化部を削除することができるためシステム規模を小さくできるという効果がある。

【００７０】

（実施の形態３）

図３は、本発明の実施の形態３における著作物保護システム３００を示す。図３において図１と同一の構成には同一の符号を付し説明を省略する。

【００７１】

著作物保護システム３００では、図２で示した著作物保護システム２００のように解読制限更新部２１２からの更新指令ＣＣをうけて暗号化装置２０１内の解読制限更新部２２３によって解読制限Ｓ１を更新するのではなく、予め暗号化装置３０１内の解読制限記憶部３１１に格納されている解読制限Ｓ１を解読制限更新部３２３によって更新する。コンテンツ鍵生成部１１７が更新された解読制限Ｓ４を用いてコンテンツ鍵ＣＫを生成し、暗号化部３１９がコンテンツＣＴの暗号化を開始することに応答して、解読制限更新部３２３は解読制限記憶部３１１に更新された解読制限Ｓ４を格納する。

【００７２】

以上のように、本実施の形態の著作物保護システム３００は、復号化装置３０２からの指令で解読制限Ｓ１を更新するのではなく、予め解読制限更新部３２３が解読制限Ｓ１を更新し、かつコンテンツ鍵生成部１１７がデータ転送鍵ＣＫを生成するので、処理ステップを短縮できるという効果がある。

【００７３】

（実施の形態４）

図４は、本発明の実施の形態４における著作権保護システム４００を示す。図４において図１と同一の構成には同一の符号を付し説明を省略する。

【００７４】

著作権保護システム４００では、時変鍵生成部４０９、４１０における時変鍵ＶＫの生成において、乱数Ｒ１、Ｒ２に加えて共通鍵ＵＫを用いる。なお、時変鍵ＶＫは、例えば、乱数Ｒ１、Ｒ２、共通鍵ＵＫを排他的論理和で結合し、一方向性関数による変換を行なって生成すればよい。

【００７５】

以上のように、本実施の形態の著作権保護システム４００によれば、外部でモニタ可能な乱数Ｒ１、Ｒ２だけから時変鍵ＶＫを生成するのではなく、秘密な共通鍵ＵＫを関連付けるようにして時変鍵ＶＫを生成しているので時変鍵ＶＫの類推が容易でなく、時変鍵ＶＫの秘匿性を向上させることができるという効果がある。

【００７６】

（実施の形態５）

図５は、本発明の実施の形態５における著作権保護システム５００を示す。図５において図１と同一の構成には同一の符号を付し説明を省略する。

【００７７】

著作権保護システム５００では、コンテンツ鍵生成部５１７、５１８におけるコンテンツ鍵ＣＫの生成において、更新された解読制限Ｓ４に加えて時変鍵ＶＫを用いる。なお、コンテンツ鍵ＣＫは、例えば、解読制限Ｓ４、時変鍵ＶＫを排他的論理和で結合し、一方向性関数による変換を行なって生成すればよい。

【００７８】

以上のように、本実施の形態の著作権保護システム５００によれば、更新された解読制限Ｓ４だけから時変鍵ＣＫを生成するのではなく、相互認証毎に時系列的に変化する時変鍵ＶＫを関連付けるようにし、時変鍵ＶＫを生成しているので、よりコンテンツの暗号化の強度を向上させることができるという効果がある。

【００７９】

（実施の形態６）

図６は、本発明の実施の形態６における著作権保護システム６００を示す。図６において図１と同一の構成には同一の符号を付し説明を省略する。

【００８０】

著作物保護システム６００では、暗号化装置６０１および復号化装置６０２に入力または出力される入出力データの全体または一部（ここでは、乱数Ｒ１、Ｒ２、応答値Ｖ１、Ｖ２、暗号化解読制限Ｓ２、Ｓ３、暗号化コンテンツＳ５）からデータ系列鍵ＴＫ１を生成するデータ系列鍵生成部６２５、６２６を暗号化装置６０１および復号化装置６０２に備える。時変鍵生成部６０９、６１０およびコンテンツ鍵生成部６１７、６１８における鍵の生成にデータ系列鍵ＴＫ１を加える。

【００８１】

なお、データ系列鍵ＴＫ１は、例えば、各入出力データのＨｉｓｌｏｒ　Ｌｏｗをカウントして生成すればよい。また、時変鍵ＶＫは、例えば、乱数Ｒ１、Ｒ２、データ系列鍵ＴＫ１を排他的論理和で結合し、一方向性関数による変換を行なって生成すればよい。また、コンテンツ鍵ＣＫは、解読制限Ｓ４、データ系列鍵ＴＫ１を排他的論理和で結合し、一方向性関数による変換を行なって生成すればよい。また、入出力される入出力データの全てからデータ系列鍵ＴＫ１を生成する必要はなく、そのうちの一部から生成するようにしてもかまわない。

【００８２】

以上のように、本実施の形態の著作権保護システム６００は、送復号化装置毎に独立に入出力される入出力データを監視し、入出力データから各機器共通なデータ系列鍵ＴＫ１を生成し、生成されたデータ系列鍵ＴＫ１を各鍵の生成に関連付けるようにしている。暗号通信の対象となる送復号化装置間で入出力データが同一である必要があるため、通信のなりすましを防止することができるという効果がある。

【００８３】

【発明の効果】

以上のように本発明に係る著作物保護システムによれば、著作物であるコンテンツの転送において、解読制限の更新情報を関連させて暗号通信を行うので、正

しく解読制限の更新処理を行わないと、コンテンツを解読できない効果がある。

【００８４】

また、本発明に係る著作物保護システムは、データ転送鍵の生成に関連する更新された解読制限を転送しなくても良いため、秘匿性を高めることができる。また、更新された解読制限の転送に係わる暗号化部、復号化部を削除することができるためシステム規模を小さくできるという効果がある。

【００８５】

また、本発明に係る著作物保護システムは、復号化装置からの指令で解読制限を更新するのではなく、予め暗号化装置が解読制限を更新し、かつデータ転送鍵を生成しているので、処理ステップを短縮できるという効果がある。

【００８６】

また、本発明に係る著作物保護システムは、外部でモニタ可能な乱数だけから時変鍵を生成するのではなく、秘密な共通鍵を関連付けるようにしているので時変鍵の類推が容易でなく、秘匿性を向上させることができるという効果がある。

【図面の簡単な説明】

【図１】

実施の形態１のシステムの構成を示す構成図である。

【図２】

実施の形態１のシステムの処理手順を示すフローチャートである。

【図３】

実施の形態２のシステムの構成を示す構成図である。

【図４】

実施の形態３のシステムの構成を示す構成図である。

【図５】

実施の形態４のシステムの構成を示す構成図である。

【図６】

実施の形態５のシステムの構成を示す構成図である。

【図７】

実施の形態６の構成を示す構成図である。

【符号の説明】

１０１、２０１、３０１、４０１、５０１、６０１　暗号化装置

１０２、２０２、３０２、４０２、５０２、６０２　復号化装置

１０３、１０４　共通鍵記憶部

１０５、１０６　乱数発生部

１０７、１０８　相互認証処理部

１０９、１１０、６０９、６１０　時変鍵生成部

１１１、２１１、３１１　解読制限記憶部

１１２、２１２、２２３、３２３　解読制限更新部

１１３、１１６、１１９　暗号化部

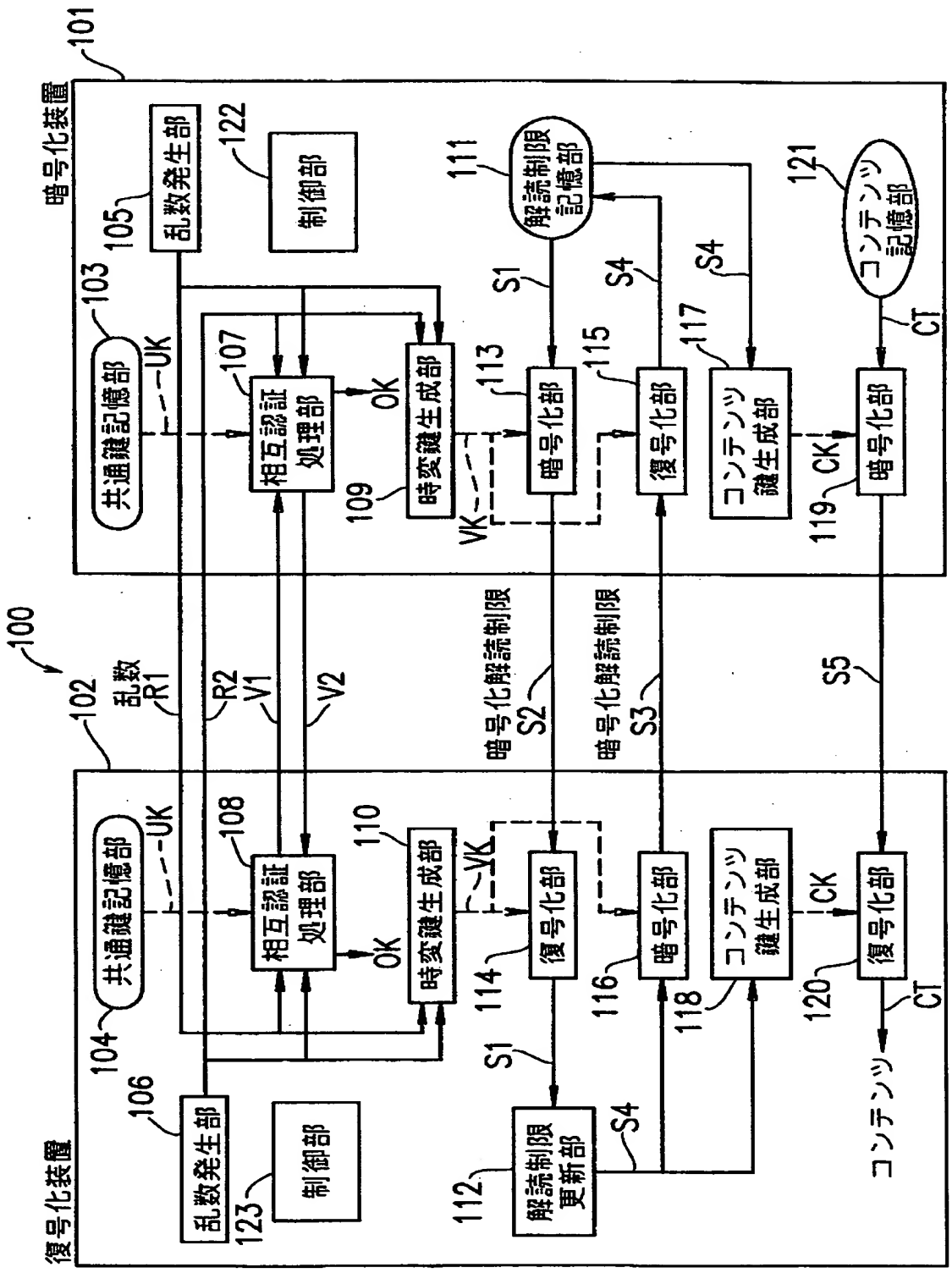
１１４、１１５、１２０　復号化部

１１７、１１８、６１７、６１８　コンテンツ鍵生成部

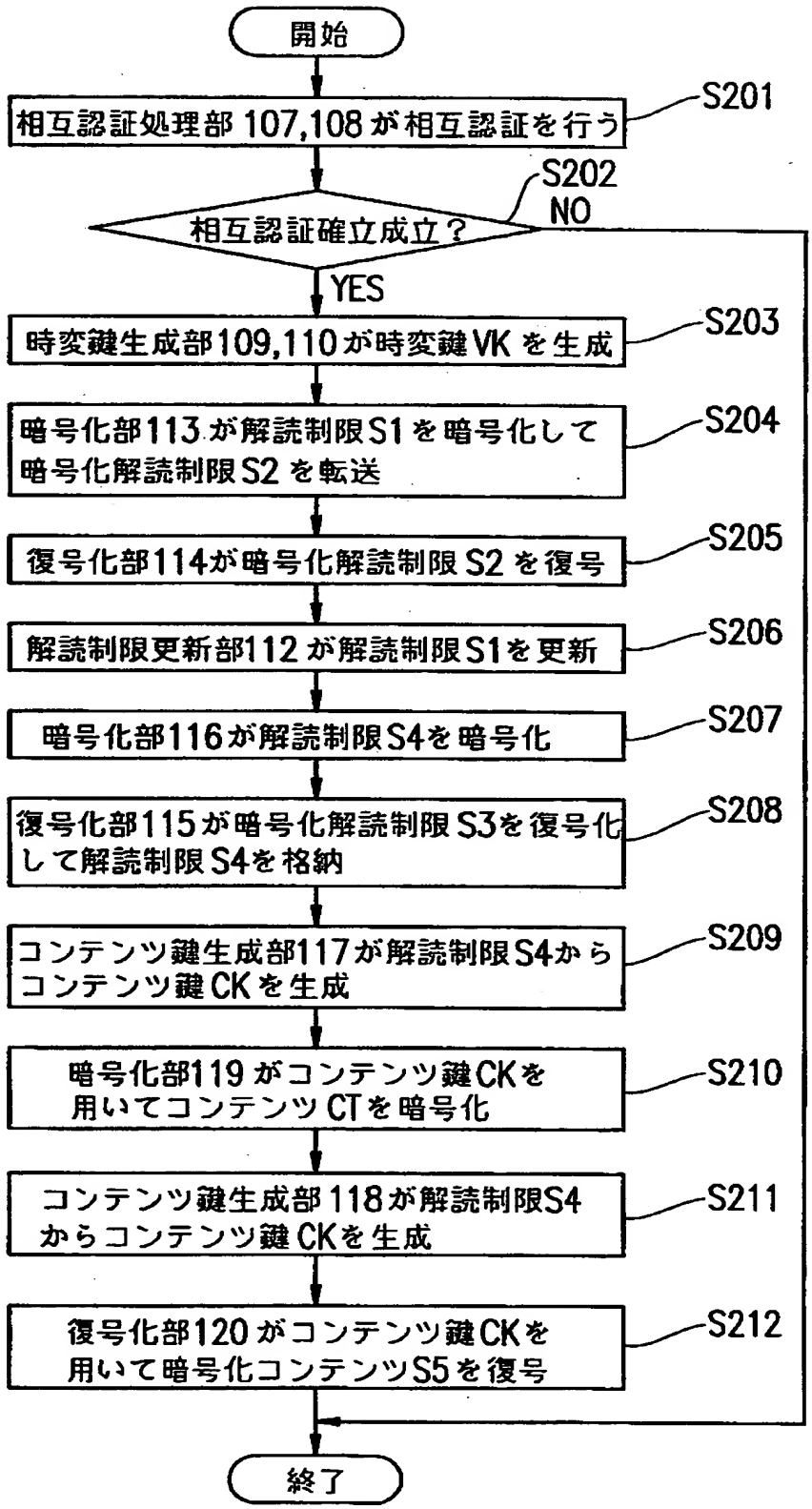
６２５、６２６　データ系列鍵生成部

【書類名】　　図面

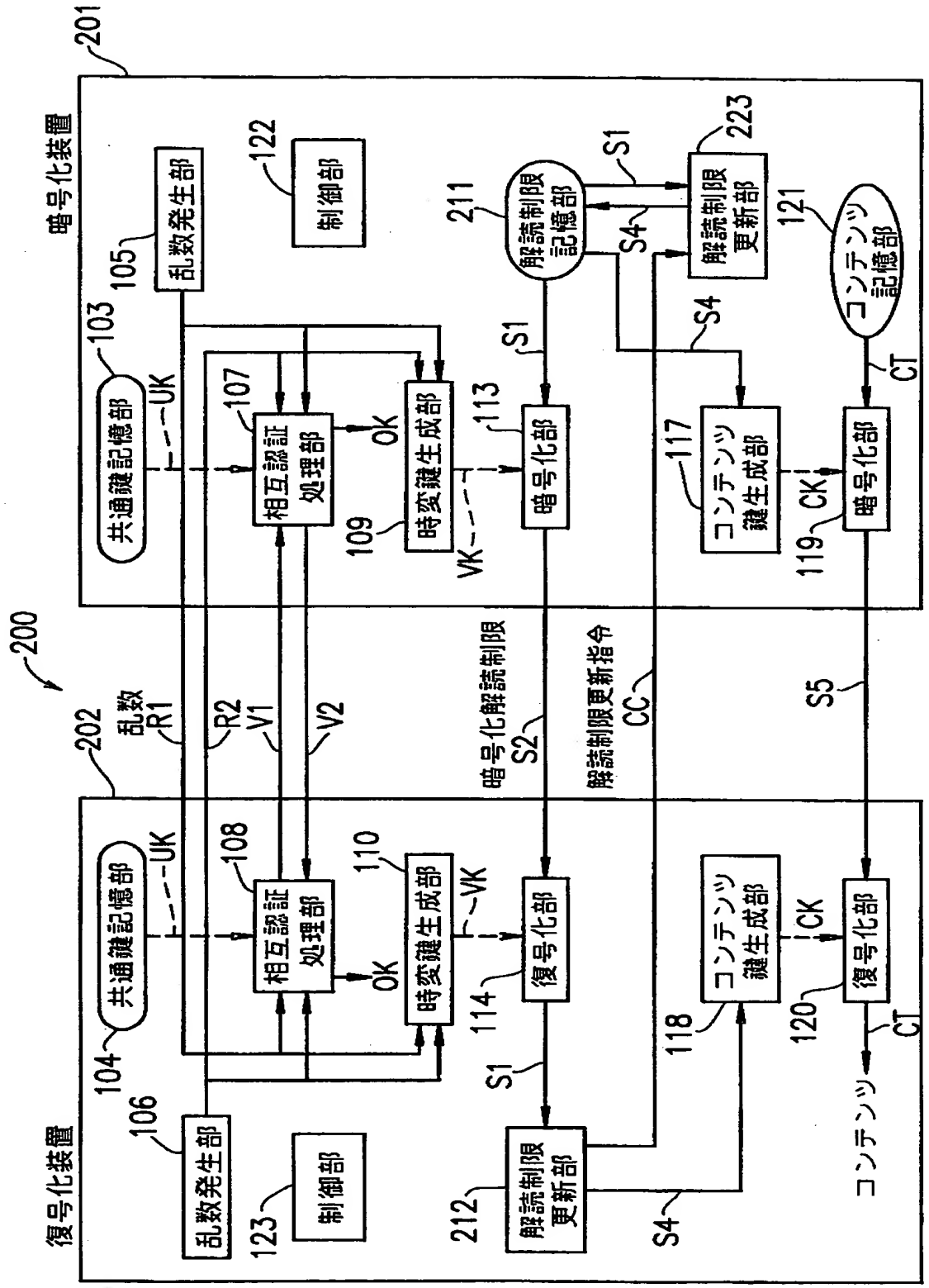
【図１】


暗号化装置
101
乱数発生部
105
制御部
122
共通鍵記憶部
103
UK
相互認証処理部
107
OK
時変鍵生成部
109
VK
暗号化部
113
復号化部
115
コンテンツ鍵生成部
117
解読制限記憶部
111
S1
S4
S4
コンテンツ記憶部
121
CT
暗号化部
119
CK
100
102
乱数
R1
R2
V1
V2
暗号化解読制限
S2
暗号化解読制限
S3
S5
復号化装置
共通鍵記憶部
104
UK
相互認証処理部
108
OK
時変鍵生成部
110
VK
復号化部
114
暗号化部
116
コンテンツ鍵生成部
118
復号化部
120
CK
CT
コンテンツ
乱数発生部
106
123
制御部
S1
解読制限更新部
112
S4

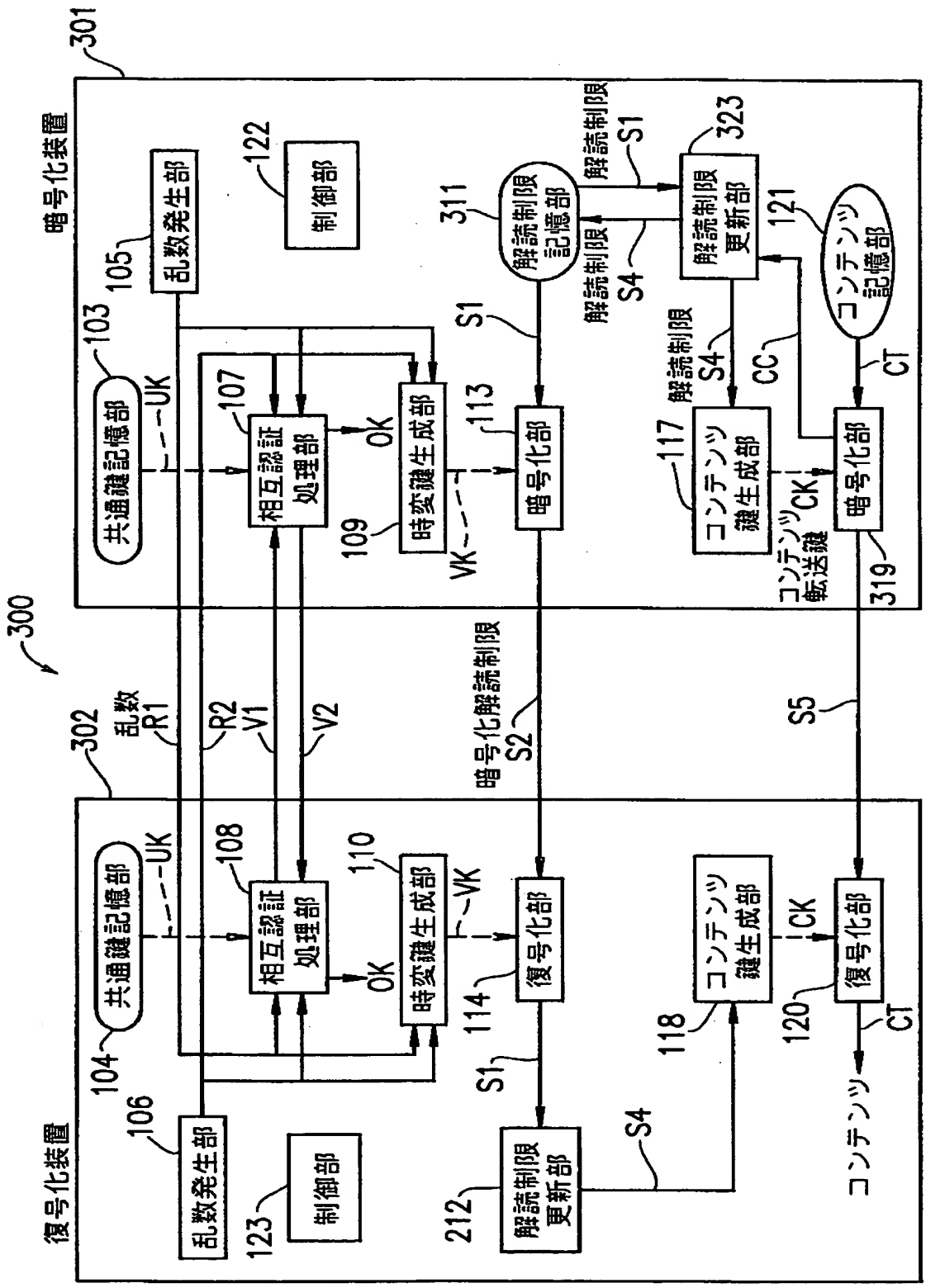
【図２】


開始
相互認証処理部107,108が相互認証を行う
S201
相互認証確立成立？
S202
NO
YES
時変鍵生成部109,110が時変鍵VKを生成
S203
暗号化部113が解読制限S1を暗号化して暗号化解読制限S2を転送
S204
復号化部114が暗号化解読制限S2を復号
S205
解読制限更新部112が解読制限S1を更新
S206
暗号化部116が解読制限S4を暗号化
S207
復号化部115が暗号化解読制限S3を復号化して解読制限S4を格納
S208
コンテンツ鍵生成部117が解読制限S4からコンテンツ鍵CKを生成
S209
暗号化部119がコンテンツ鍵CKを用いてコンテンツCTを暗号化
S210
コンテンツ鍵生成部118が解読制限S4からコンテンツ鍵CKを生成
S211
復号化部120がコンテンツ鍵CKを用いて暗号化コンテンツS5を復号
S212
終了

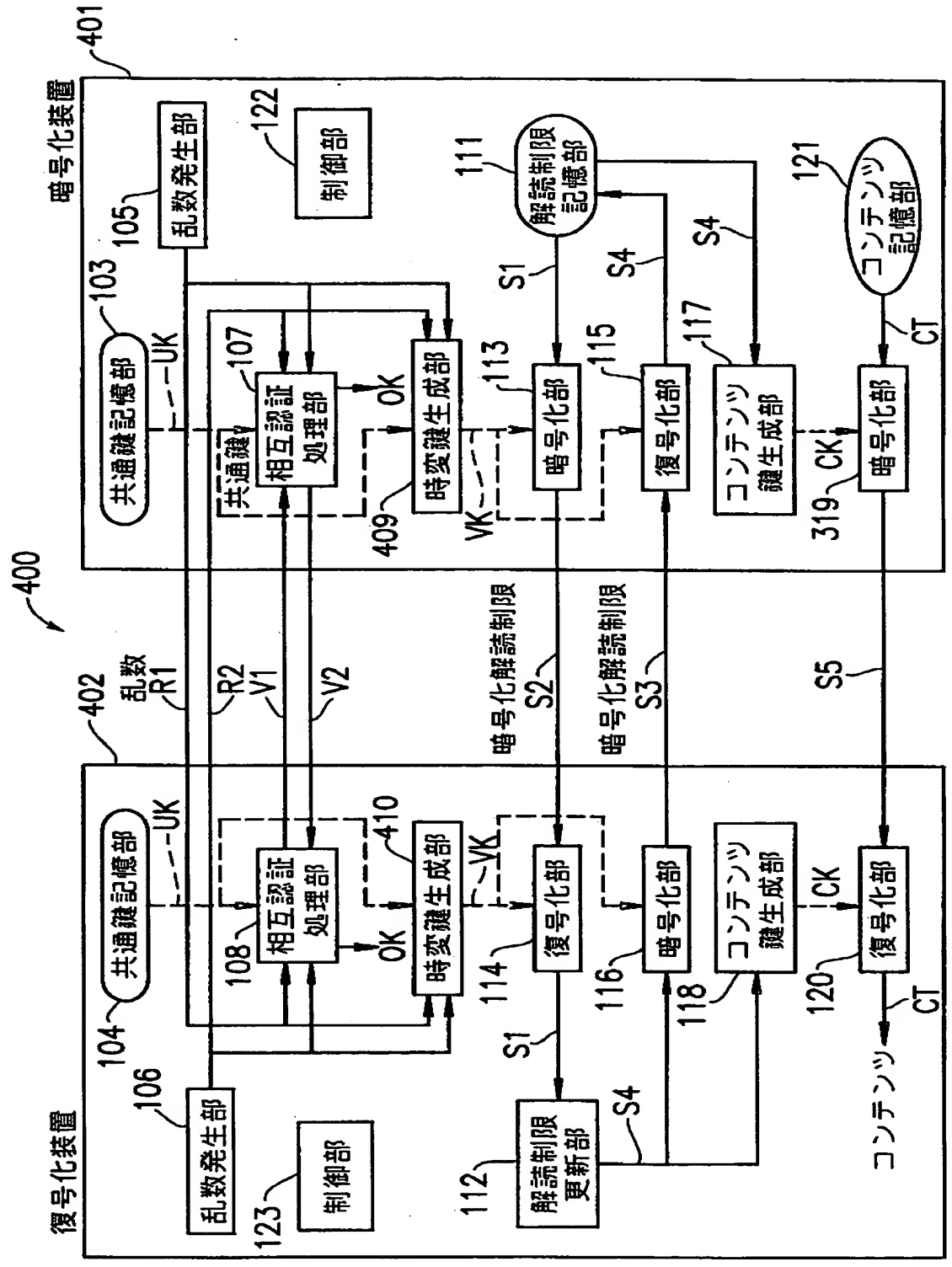
【図３】


200
暗号化装置
201
乱数発生部
105
制御部
122
共通鍵記憶部
103
UK
相互認証処理部
107
OK
時変鍵生成部
109
VK
暗号化部
113
解読制限記憶部
211
解読制限更新部
223
S1
S4
コンテンツ記憶部
121
CT
コンテンツ鍵生成部
117
CK
暗号化部
119
乱数
R1
R2
V1
V2
暗号化解読制限
S2
解読制限更新指令
CC
S5
202
復号化装置
共通鍵記憶部
104
UK
相互認証処理部
108
OK
時変鍵生成部
110
VK
復号化部
114
S1
コンテンツ鍵生成部
118
CK
復号化部
120
CT
コンテンツ
乱数発生部
106
制御部
123
解読制限更新部
212
S4

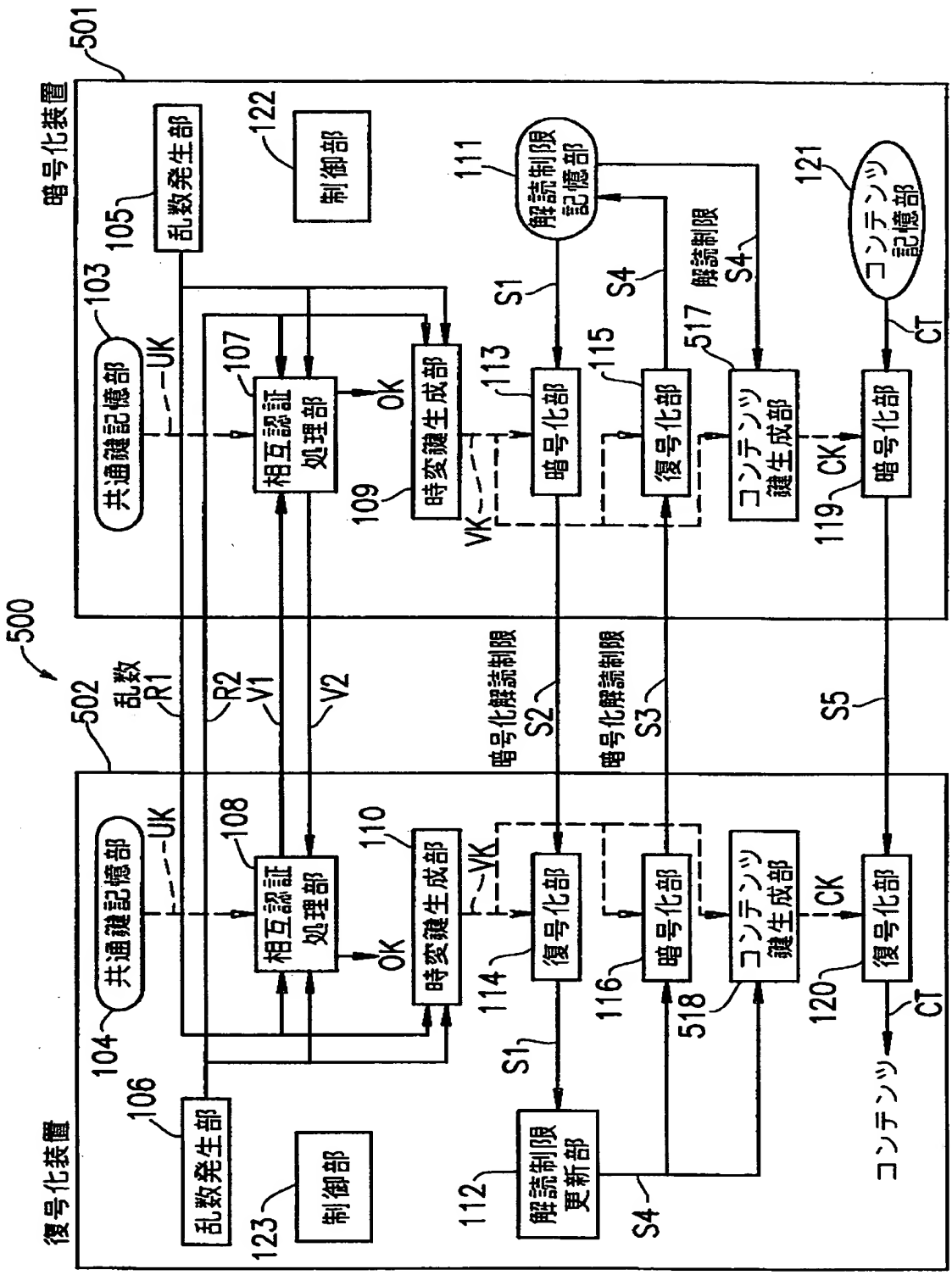
【図４】


暗号化装置
301
乱数発生部
105
制御部
122
共通鍵記憶部
103
UK
相互認証処理部
107
OK
時変鍵生成部
109
113
VK
暗号化部
S1
解読制限記憶部
311
解読制限
S1
解読制限更新部
323
解読制限
S4
S4
コンテンツ記憶部
121
CC
CT
解読制限
S4
コンテンツ鍵生成部
117
CK
コンテンツ転送鍵
暗号化部
319
300
乱数
R1
R2
V1
V2
302
暗号化解読制限
S2
S5
復号化装置
共通鍵記憶部
104
UK
相互認証処理部
108
OK
時変鍵生成部
110
VK
復号化部
114
S1
コンテンツ鍵生成部
118
CK
復号化部
120
CT
コンテンツ
乱数発生部
106
制御部
123
解読制限更新部
212
S4

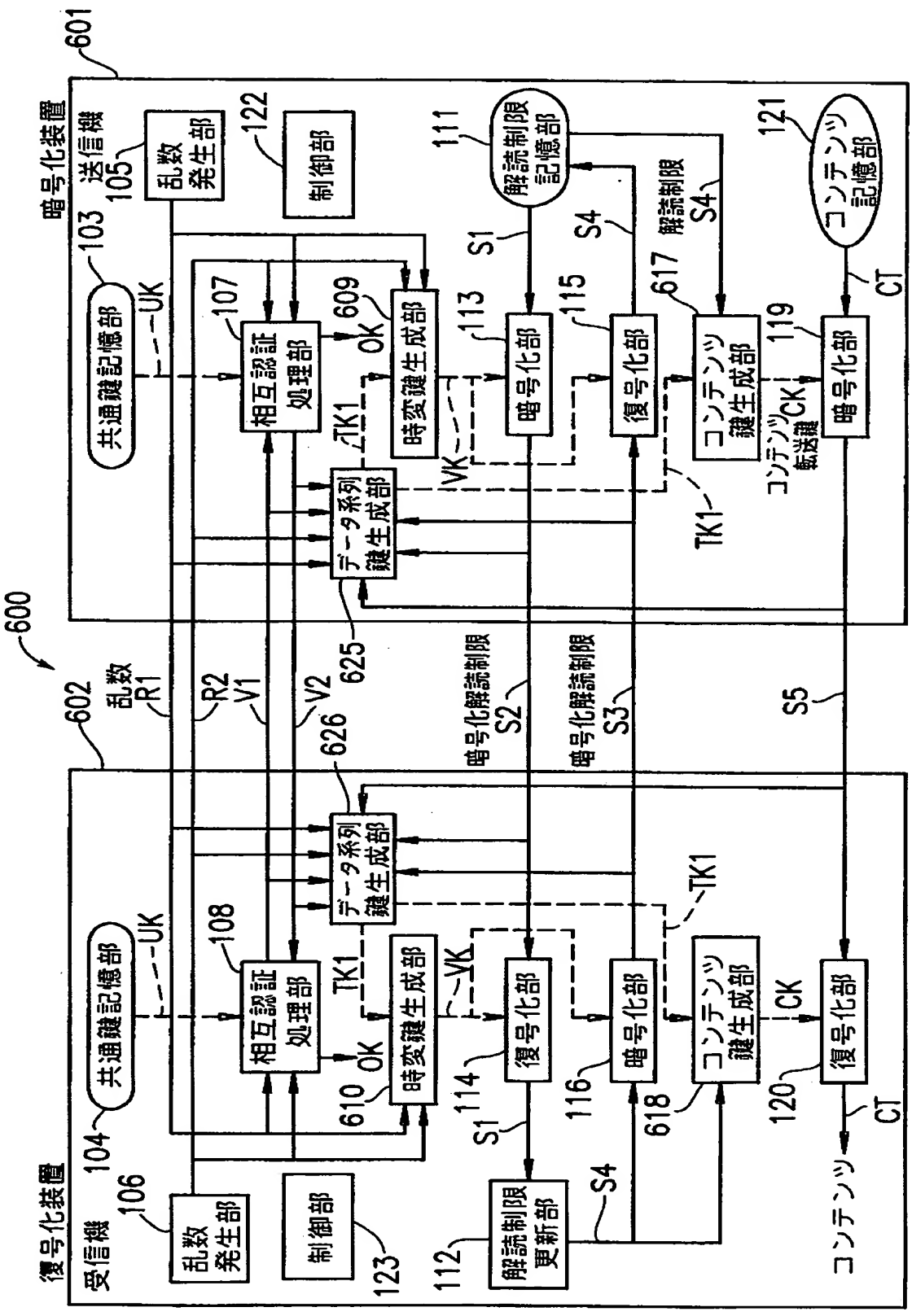
【図５】


400
暗号化装置
401
乱数発生部
105
制御部
122
共通鍵記憶部
103
UK
相互認証処理部
107
共通鍵
OK
時変鍵生成部
409
VK
暗号化部
113
解読制限記憶部
111
S1
復号化部
115
S4
コンテンツ鍵生成部
117
S4
コンテンツ記憶部
121
暗号化部
319
CK
CT
乱数
R1
R2
V1
V2
暗号化解読制限
S2
暗号化解読制限
S3
S5
402
復号化装置
共通鍵記憶部
104
UK
相互認証処理部
108
410
時変鍵生成部
VK
復号化部
114
S1
暗号化部
116
コンテンツ鍵生成部
118
CK
復号化部
120
CT
コンテンツ
乱数発生部
106
制御部
123
解読制限更新部
112
S4

【図６】


暗号化装置
501
乱数発生部
105
制御部
122
共通鍵記憶部
103
UK
相互認証処理部
107
OK
時変鍵生成部
109
VK
暗号化部
113
復号化部
115
解読制限記憶部
111
S1
S4
解読制限
517
S4
コンテンツ鍵生成部
コンテンツ記憶部
121
CT
CK
暗号化部
119
500
502
乱数
R1
R2
V1
V2
暗号化解読制限
S2
暗号化解読制限
S3
S5
共通鍵記憶部
104
UK
相互認証処理部
108
OK
時変鍵生成部
110
VK
復号化部
114
暗号化部
116
コンテンツ鍵生成部
518
CK
復号化部
120
CT
コンテンツ
S1
乱数発生部
106
制御部
123
解読制限更新部
112
S4
復号化装置

【図７】


暗号化装置
601
送信機
乱数発生部
105
制御部
122
解読制限記憶部
111
共通鍵記憶部
103
UK
相互認証処理部
107
609
OK
時変鍵生成部
113
暗号化部
115
復号化部
617
解読制限
S4
コンテンツ鍵生成部
119
コンテンツ記憶部
121
CT
S1
TK1
VK
データ系列鍵生成部
600
602
乱数
R1
R2
V1
V2
625
626
暗号化解読制限
S2
暗号化解読制限
S3
S5
受信機
104
106
108
610
114
116
618
120
112
123
復号化部
暗号化部
コンテンツ鍵生成部
CK
コンテンツ
解読制限更新部
制御部
乱数発生部
コンテンツ転送鍵
復号化装置

【書類名】要約書

【要約】

【課題】　記録媒体に記録された解読制限を持ったディジタルコンテンツの不正解読を防止するシステムを提供する。

【解決手段】　コンテンツ鍵の共有化とそのコンテンツ鍵を用いた暗号通信を行う暗号化装置および復号化装置から構成される通信システムにおいて、暗号化装置及び復号化装置は相互認証によって相手機器が正当な機器であることを認証し合い、かつ相互認証に用いた乱数から時変鍵を共有化する。復号化装置に格納されている再生回数データなどの解読制限を時変鍵で暗号化し、機密保護した状態で暗号化装置に転送し、かつ両機器において解読制限の更新を行い解読制限を共有化する。コンテンツのロードに際しては、更新された解読制限から生成したコンテンツ鍵を用いて暗号通信を行う構成とした。

【選択図】　図４

出証特２０００－３１１２８７７

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社